AD-A102 460 NAVAL OCEAN SYSTEMS CENTER SAN DIEGO CA F/G 9/5
FUTURE DIRECTIONS IN NAVY ELECTRONIC SYSTEM RELIABILITY AND SUR--ETC(U)
JUN 81 M VINEBERG, R D PETERSON
UNCLASSIFIED NOSC/TD-448 NL

1 of 1
AD
A102460

END
DATE
FILMED
9-81
DTIC

LEVEL II

(12)

NOSC

NOSC TD 448

NOSC TD 448

Technical Document 448

FUTURE DIRECTIONS IN NAVY ELECTRONIC SYSTEM RELIABILITY AND SURVIVABILITY

Maniel Vineberg
Reeve D. Peterson

June 1981

Prepared for
Naval Electronic Systems Command
(NAVELEX 614)

Approved for public release; distribution unlimited

NAVAL OCEAN SYSTEMS CENTER
SAN DIEGO, CALIFORNIA 92152

NAVAL OCEAN SYSTEMS CENTER, SAN DIEGO, CA 92152

AN ACTIVITY OF THE NAVAL MATERIAL COMMAND

ADMINISTRATIVE INFORMATION

The work was performed by members of the Micro-Electronics Technology and Applications Division under program element 62762N, project EC01, and subproject XF62582094.

Released by
O.H. Lindberg, Head
Micro-Electronics Technology
and Applications Division

Under authority of
P.C. Fletcher, Head
Electronics Engineering and
Sciences Department

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

14 NOSC/T...-448

9 REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
NOSC Technical Document 448 (TD 448)

2. GOVT ACCESSION NO.
AD-A102460

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
6 FUTURE DIRECTIONS IN NAVY ELECTRONIC SYSTEM RELIABILITY AND SURVIVABILITY

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
10 Maniel Vineberg
Reeve D. Peterson

12 17

8. CONTRACT OR GRANT NUMBER(s)

17

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Ocean Systems Center
San Diego, CA 92152

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
62762N, EC01, XF62582094

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Electronic Systems Command (NAVELEX 614)
Washington, DC 20360

11

12. REPORT DATE
Jun[illegible]981

13. NUMBER OF PAGES
10

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

16 F62582

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Electronic systems	Very Large Scale Integration (VSLI)
Reliability	Networking
Survivability	
Scheduled maintenance	
Fault tolerance	

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The rapid expansion of the threat to US Naval forces has made complex sensor systems and combat direction systems indispensable to the Fleet. Increasing complexity has led to decreasing reliability, which results in degraded Fleet readiness and morale as well as increased logistics and maintenance costs. A scheduled-maintenance policy is proposed as one remedy to these problems. To implement this policy, electronic systems which are very reliable and which include health and readiness monitoring capability must be developed. Fault tolerance is one discipline for the design of such systems. Very Large Scale Integration (VLSI) will provide a cost-effective integrated circuit technology from which to build fault-tolerant systems. Navy ships and task groups must be able to continue

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

393159 DU

20. ABSTRACT (Continued)

operation in spite of partial losses; this implies a need to distribute vital data, data-processing capability, and communication capability through the use of intraship and intership networks. The capability to build electronic equipment that requires only scheduled maintenance and that is survivable through networking will be realized through (1) definition of a framework for the specification of reliability, monitoring and survivability requirements, and costs; (2) capture of reliable system design techniques; (3) development of a survivable-network design methodology; and (4) development of an electronic system design facility.

CONTENTS

1.0 INTRODUCTION

Technology may be "pushed" by the efforts of self-motivated basic researchers or "pulled" by the needs of society. In the area of reliable computing there is precedence for the latter, especially as those needs have been manifested by the US Government. The STAR (Self-Testing And Repairing) computer[1] was built at the Jet Propulsion Laboratory in response to the reliability requirements of spaceborne computers. Likewise, the SIFT (Software Implemented Fault Tolerance) computer[2] at SRI International and the FTMP (Fault-Tolerant Multiprocessor[3] at the Charles Stark Draper Laboratory were built in response to requirements, defined by NASA, to control dynamically unstable aircraft. The basis for the very high reliability of these computers is fault tolerance; ie, correct operation in the presence of faults. The primary tool for achieving fault tolerance is hardware redundancy.[4]

Very Large Scale Integration (VLSI)[5] is an emerging semiconductor technology. The Department of Defense is actively encouraging VLSI research through its Very High Speed Integrated Circuits (VHSIC) program.[6] VLSI circuitry holds the promise of increased system reliability since greater component density will decrease the number of (relatively unreliable) interconnections between integrated circuit chips. Since the increased density will also decrease the cost of hardware redundancy, VLSI will provide a cost-effective basis for applying fault-tolerant design techniques to Navy system reliability problems.[7] Therefore, fault-tolerant design research is being actively pursued under the VHSIC program.[8-10]

The rapid expansion of threat to US Naval forces has been well documented.[11-14] The number and dispersal as well as the capability and sophistication of potentially hostile forces continue to grow very rapidly. The response times to potential attack have already

---

1. Avizienis, A., et al, The STAR (Self-Testing and Repairing) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design, IEEE Trans on Computers, v C-20, no 11, Nov 1971, p 1312-1321.
2. Wensley, J., et al, SIFT: The Design and Analysis of a Fault-Tolerant Computer for Aircraft Control, Proc IEEE, v 66, no 10, Oct 1978, p 1240-1255.
3. Hopkins, A., et al, FTMP – A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft, Proc IEEE, v 66, no 10, Oct 1978, p 1221-1239.
4. Avizienis, A., Fault-Tolerant Systems, IEEE Trans on Computers, v C-25, no 12, Dec 1976, p 1304-1312.
5. Mead, C., and L. Conway, Introduction to VLSI Systems, Addison-Wesley, Reading MA, 1979.
6. Davis, R., The DoD Initiative in Integrated Circuits, Computer, v 12, no 7, July 1979, p 74-79.
7. Peterson, R., Fault Tolerance for Military Systems, EASCON 80 Record, IEEE Electronics and Aerospace Systems Conventions, Arlington VA, p 410-412.
8. Kautz, W., and J. Goldberg, Fault Tolerant Architecture for VHSIC, Quarterly Technical Report (Sep - Nov 1980), SRI International, Menlo Park, 10 Feb 1981.
9. Abraham, J., et al, Reliable, High-Performance VHSIC Systems, Quarterly Progress Report 2 (Nov 1980 - Jan 1981), Coordinated Science Laboratory, University of Illinois, Urbana, 1981.
10. Clary, J., et al, The Identification and Assessment of On-Chip Self-Test and Repair Techniques, VHSIC - Phase III, Quarterly Report, Systems and Measurements Division, Research Triangle Institute, Research Triangle Park, Jan 1981.
11. Simmons, H., The US Navy Countering the Soviet Buildup, International Defense Review, Special Series (Warships and Naval Systems), 1976, p 5-9.
12. Edwards, M., Soviet Expansion and Control of the Sea-Lanes, United States Naval Institute Proceedings, v 106/9/931, Sep 1980, p 46-51.
13. Booda, L., Soviet Sea Technology Shows Muscle, Sea Technology, v 21, no 7, July 1980, p 7.
14. Wall, P., The Planned Destruction of the West, Sea Power, v 22, no 11, Nov 1979, p 17-22.

decreased to the point that computer-based sensor, fire-control, and combat direction systems are indispensable to the Fleet. Because of the rapid increase in the number and complexity of functions which they must perform, these systems are increasingly complex, expensive, and unreliable.[15] Unreliable systems pose special problems for the Navy; they are often unavailable for use, degrading Fleet combat readiness and causing personnel morale problems; they require local inventories of spare parts; and they require frequent attention from well trained onboard maintenance personnel, who are in extremely short supply.[16,17] If unchecked, life-cycle costs associated with computer systems will continue to increase rapidly. In addition, the increasing complexity of new systems will introduce new sources of error and new maintenance difficulties.[18] The situation just described highlights two Navy requirements: (1) improve operational readiness; and (2) reduce maintenance costs.

During combat, a damaged ship may lose one or more electronic systems. Physical distribution can alleviate the effects of this damage. Intraship networks which degrade gracefully (that is, which contain the damage and continue to provide some support) are necessary to the survival of the ship's capability. Ships are generally organized into task groups to carry out specific assignments. A group must be able to complete its assignment in spite of losses. Vital data, data-processing capability, and communication capability must be replicated and distributed throughout the task group to reduce the probability of failure when equipment is destroyed. This represents a requirement for survivable intership networks. Other justifications for the development of such networks include opportunities for load sharing, concurrent processing, and rapid transfer of data and capability.

2.0 OBJECTIVES

The requirements to improve operational readiness and reduce maintenance costs can be partially met by building more reliable electronic systems. This will allow the Navy to institute a policy of "scheduled maintenance." This policy implies "maintenance-free" missions during which systems operate without maintenance, to be serviced (for example) only when the ships themselves return to port. Scheduled maintenance has not been feasible in the past because existing technology would not support such a policy. However, with today's technology, systems can be designed to be fault-tolerant; faulty system components would be replaced at the regular service intervals. A scheduled-maintenance policy would represent a significant savings over the current practice of providing spare parts and onboard technicians to fix systems when they fail.

While they are expected to be more reliable than present systems, new Navy electronic systems will still fail on occasion. As they do now, system failures will result in loss of capability and may lead to aborted missions. The number and types of faults which would accumulate in a fault-tolerant system would provide an indication of the "health" of that system, as system redundancy were reduced or compromised by faults, the margin of safety

---

15. Aerospace Daily, Navy Data Show Systems with High Failure Rates, Low Availability, 17 Feb 1981, p 234.
16. Mossberg, W., Big Carrier Illustrates Manpower Difficulties Afflicting US Forces, Wall Street Journal, 30 Oct 1980, p 1, 14.
17. Hessman, J., Military Personnel Problems Reach Crisis Stage, Sea Power, v 23, no 3, Mar 1980, p 23-28.
18. Fink, D., Military Stresses Maintainability, Reliability, Aviation Week, v 113, no 14, 6 Oct 1980, p 42-43.

would decrease and the likelihood of system failure would increase. For this reason, a health and readiness monitoring capability (that is, a capability to monitor the accumulated faults) must be incorporated into new systems. This capability would support the scheduled-maintenance policy: unhealthy systems could be upgraded at unscheduled times if necessary (by a minimal onboard maintenance crew, a mobile maintenance crew, remote communication, or some other cost-effective method). The system health and readiness monitoring capability would be part of a larger capability to assess ship, task group, and Fleet readiness.

The requirement for survivable networks can be partially met through such techniques as replicated functions, multiple copies of system data and programs, multiple communication paths, and distributed recovery mechanisms. In general, loss of capability because of internal failure will affect a system in the same way as loss because of hostile action. Therefore, meeting the requirement for survivable systems will support the scheduled-maintenance policy.

The primary reliability and survivability objectives are: (1) to produce Navy electronic systems which are very reliable, incorporate health and readiness monitoring, and can therefore be covered by a scheduled-maintenance policy; and (2) to formulate a survivable-network design methodology.

3.0 APPROACH

The approach to meeting scheduled-maintenance and survivability objectives will be to: (1) define a framework for the specification of Navy electronic system reliability, monitoring and survivability requirements, and costs; (2) identify issues relevant to the design of survivable networks; (3) capture existing techniques and methods where possible and support research where necessary to address Navy requirements and network design issues; (4) demonstrate feasibility; and (5) build a design support facility.

3.1 REQUIREMENTS

The first step in defining Navy electronic system reliability, monitoring, and survivability requirements is to bound the scope of the effort. Current Navy ships carry a variety of electronic systems including computers local to weapons and sensors; message and data-processing systems; signal-processing systems; fire-control systems; and command, control, and communication systems. Eventually, these systems will be linked within intraship networks which will, in turn, be linked within intership networks. The scope of the effort must include all elements of an intership network.

The second step is to construct a hierarchical framework to expose tradeoffs between reliability, monitoring, and survivability requirements and costs. For example, a given network reliability requirement might be met through various combinations of node and link reliabilities at various relative costs. Likewise, the reliability requirements of a given system (node) might be met through various subsystem configurations. In practice, cost constraints would probably be given and then the various requirements cited above would be traded against performance and physical requirements (not discussed here).

Once a hierarchical framework is in place, the process of formulating requirements for specific systems can begin. For reliability, mean-time-to-failure requirements and confidence levels (ie, the percentage of systems likely to meet requirements) will be needed. For monitoring, specifications of the smallest replaceable unit, the types of faults to be detected, and the type of indications to be provided will be needed. For survivability, definitions of critical data, data-processing capability, and communications capability will be needed.

Cost constraints will be an important factor in determining the system reliabilities and confidence levels that are achievable. A "Maintenance Free Mission Analysis"[19] provides an example calculation of savings (from current costs) expected to accrue to a submarine as a result of introducing four specific maintenance-free systems: ECM, navigation, sonar, and fire control. This type of analysis will help to establish initial estimates of savings which will, in turn, partially establish cost constraints. The cost of providing a given reliability for a system is related to the fault set (the expected types of failures) of that system. A preliminary indication of typical requirements and costs will come from examinations of existing and new systems.

3.2 NETWORK DESIGN ISSUES

The development of efficient, survivable networks will be based on a number of technologies. Navy intraship and intership networks will first be specified in sufficient detail to allow these technologies to be identified. Research and development will then be initiated as a set of independent efforts within the framework of the high-level specifications. Such areas as network protocols, data formats, distributed databases, and communications media will receive early attention. An important goal of these early efforts will be to establish standard protocols, formats, interfaces, and programming languages. These will focus subsequent research and development and will provide a flexible framework for early network design and subsequent implementation, growth, and improvement.

The Naval Ocean Systems Center (NOSC) is cooperating with the Marine Corps, whose Mobile Command Concept[20] provides the basis for a computer network.

3.3 TECHNIQUES AND METHODS

A broad range of techniques and methods, from manned intervention to total automation, will be available to address Navy reliability and monitoring requirements. Existing reliable-computing design and analysis methods and techniques will be surveyed. This is important for several reasons: (1) It will educate Navy electronic-system developers to the state-of-the-art in reliable-system technology and to the general availability of solutions to reliability problems; (2) It will serve as a first step in the migration of techniques (from wherever they are discovered) into the Navy repertoire; and (3) It will provide a guide (along with requirements) to what research and development must be initiated to meet Navy requirements.

It is important that all techniques and methods which are covered by this survey be understood and reported within the context of the requirements to which they respond. This will help Navy designers to understand the possible applications of these techniques and methods to Navy systems. It is clear to researchers[21] that the design of reliable systems is an art and that successful design responds directly to requirements.

---

19. Control Data Corporation, Professional Services Division, Maintenance Free Mission Analysis, Informal Technical Report, 1 Apr 1977.
20. NOSC Technical Document 345, Marine Corps Mobile Command Concept (MCC): Functional Interface Analysis, by D. Leonard et al, 1 July 1980.
21. Hopkins, A., Fault-Tolerant System Design: Broad Brush and Fine Print, Computer, v 13, no 3, Mar 1980, p 39-45.

Existing techniques and methods will not be sufficient to meet all Navy system reliability and monitoring requirements. For example, fault-tolerant design techniques appropriate to VLSI technology are not expected to be identical to techniques used for earlier technologies. The VHSIC program is expected to shed light on this and other issues regarding the emerging VLSI technology. NOSC is currently assessing the suitability of fault-tolerant techniques and VLSI to address digital circuit reliability requirements.

Where necessary, new research will be initiated and ongoing research encouraged, either by direct effort or by the channeling of funds, to develop reliable-design methods and techniques. To assure that limited Navy resources are directed toward areas of greatest need, all research support must be based on a thorough understanding of Navy requirements, a familiarity with existing methods and techniques, and an awareness of related research and development efforts. To increase the probability of success (and decrease the probability of redundant effort), NOSC is cooperating with the Air Force, in particular with members of the Autonomous Spacecraft Maintenance (ASM) Study Group.[22] The objectives and constraints of the ASM effort appear to complement Navy objectives and constraints. (Completely autonomous spaceborne systems are to be built, but the possible need for communications from the ground is recognized.)

3.4 FEASIBILITY

To assure a continued Navy commitment to the specification, design, development, and deployment of electronic systems which meet reliability, monitoring, and survivability requirements, the feasibility of designing and developing such systems must be demonstrated. The first step, designing reliable computer systems, may appear to have already been taken. Indeed, fault-tolerant computers have been designed and built for several applications. However, it has yet to be shown that reliable computer systems can be designed to address the wide range of Navy reliability and performance requirements. Tools will be developed which support the reliability aspect of the design process. These tools will free the designer from reliability considerations, thereby allowing him to focus on system applications. Demonstration of such tools would indicate that reliable systems can be designed cost effectively.

The second step, developing and testing a "typical" system, is intended to achieve early, demonstrable results. A system component (for example, a standard Navy tactical computer) will be selected, designed, modeled, and built to meet certain reliability and monitoring requirements. Provision will also be made to demonstrate that the component could meet all accepted performance requirements, cost constraints, and physical constraints (power use, size, weight, etc). It is expected that existing techniques[23] will be used to adapt off-the-shelf equipment to the task (see also references 8-10).

Support tools as well as software and hardware models of the reliable component will be demonstrated to various Navy groups. This will alert sponsors and designers to the feasibility of designing and building electronic systems which meet the reliability and monitoring requirements necessary to implement a scheduled-maintenance policy.

---

22. Jet Propulsion Laboratory, Final Report of the Autonomous Spacecraft Maintenance Study Group, prepared for the Air Force Office of Scientific Research, Dec 1980.

23. Rennels, D., Distributed Fault-Tolerant Computer Systems, Computer, v 13, no 3, Mar 1980, p 55-65.

3.5 DESIGN SUPPORT FACILITY

A facility will be built to support a wide range of system development activities, such as requirements and functional specification, design, modeling, test, etc. It will serve as a collection point for tools which support the design of reliable electronic systems and survivable networks. These tools will be tested and integrated into a comprehensive design facility. The facility will be most useful if it is easy to use, modify, and transport. The magnitude of this endeavor makes it desirable to pool resources and results with other interested groups.

4.0 SUMMARY

A generation from now, the Navy systems of today will seem antiquated. That electronic systems actually failed "in those days" will be a phenomenon to be contemplated with wonder. The young will find it astounding that people had to be on hand to maintain such systems and that, in spite of their presence, the systems still experienced failures and resulting down time. They will be surprised to learn that one failure at a "critical" point could cripple an entire system.

If this is in fact to be the view from a generation hence, however, new directions must be taken today. Needs can be met only if they are clearly identified and recognized as important. General needs must be translated into specific requirements and those requirements must be considered within a framework which exposes design and cost tradeoffs. A policy of scheduled maintenance will give rise to specific system reliability as well as health and readiness monitoring requirements. The need for survivable systems must be translated into well defined requirements for intraship and intership computer networks. Existing reliable computer system design techniques must be integrated into a design facility which supports the design of systems that meet those requirements. Where this is not yet possible, the Navy must "pull" technology.

REFERENCES

1. Avizienis, A., et al, The STAR (Self-Testing and Repairing) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design, IEEE Trans on Computers, v C-20, no 11, Nov 1971, p 1312-1321.

2. Wensley, J., et al, SIFT: The Design and Analysis of a Fault-Tolerant Computer for Aircraft Control, Proc IEEE, v 66, no 10, Oct 1978, p 1240-1255.

3. Hopkins, A., et al, FTMP – A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft, Proc IEEE, v 66, no 10, Oct 1978, p 1221-1239.

4. Avizienis, A., Fault-Tolerant Systems, IEEE Trans on Computers, v C-25, no 12, Dec 1976, p 1304-1312.

5. Mead, C., and L. Conway, Introduction to VLSI Systems, Addition-Wesley, Reading MA, 1979.

6. Davis, R., The DoD Initiative in Integrated Circuits, Computer, v 12, no 7, July 1979, p 74-79.

7. Peterson, R., Fault Tolerance for Military Systems, EASCON 80 Record, IEEE Electronics and Aerospace Systems Conventions, Arlington VA, p 410-412.

8. Kautz, W., and J. Goldberg, Fault Tolerant Architecture for VHSIC, Quarterly Technical Report (Sep–Nov 1980), SRI International, Menlo Park, 10 Feb 1981.

9. Abraham, J., et al, Reliable, High-Performance VHSIC Systems, Quarterly Progress Report 2 (Nov 1980–Jan 1981), Coordinated Science Laboratory, University of Illinois, Urbana, 1981.

10. Clary, J., et al, The Identification and Assessment of On-Chip Self-Test and Repair Techniques, VHSIC – Phase III, Quarterly Report, Systems and Measurements Division, Research Triangle Institute, Research Triangle Park, Jan 1981.

11. Simmons, H., The US Navy – Countering the Soviet Buildup, International Defense Review, Special Series (Warships and Naval Systems), 1976, p 5-9.

12. Edwards, M., Soviet Expansion and Control of the Sea-Lanes, United States Naval Institute Proceedings, v 106/9/931, Sep 1980, p 46-51.

13. Booda, L., Soviet Sea Technology Shows Muscle, Sea Technology, v 21, no 7, July 1980, p 7.

14. Wall, P., The Planned Destruction of the West, Sea Power, v 22, no 11, Nov 1979, p 17-22.

15. Aerospace Daily, Navy Data Show Systems with High Failure Rates, Low Availability, 17 Feb 1981, p 234.

16. Mossberg, W., Big Carrier Illustrates Manpower Difficulties Afflicting US Forces, Wall Street Journal, 30 Oct 1980, p 1, 14.

17. Hessman, J., Military Personnel Problems Reach Crisis Stage, Sea Power, v 23, no 3, Mar 1980, p 23-28.

18. Fink, D., Military Stresses Maintainability, Reliability, Aviation Week, v 113, no 14, 6 Oct 1980, p 42-43.

19. Control Data Corporation, Professional Services Division, Maintenance Free Mission Analysis, Informal Technical Report, 1 Apr 1977.

20. NOSC Technical Document 345, Marine Corps Mobile Command Concept (MCC): Functional Interface Analysis, by D. Leonard et al, 1 July 1980.

21. Hopkins, A., Fault-Tolerant System Design: Broad Brush and Fine Print, Computer, v 13, no 3, Mar 1980, p 39-45.

22. Jet Propulsion Laboratory, Final Report of the Autonomous Spacecraft Maintenance Study Group, prepared for the Air Force Office of Scientific Research, Dec 1980.

23. Rennels, D., Distributed Fault-Tolerant Computer Systems, Computer, v 13, no 3, Mar 1980, p 55-65.